# Blockchain: A Panacea for Electronic Health Records?

Mohamad Kassab[1], Joanna DeFranco[1], Tarek Malas[2], Valdemar Vicente Graciano Neto[3], Giuseppe Destefanis[4]

[1]*Pennsylvania State University*, Malvern, PA, U.S.A.
{muk36, jfd104}@psu.edu

[2]*Institut Universitaire de Cardiologie et Pulmonologie de Québec (IUCPQ)*, Québec City, Canada
tarek.malas@gmail.com

[3]*Universidade Federal de Goiás*, Goiânia, Brazil
valdemarneto@inf.ufg.br

[4]*Brunel University*, London, U.K.
giuseppe.destefanis@brunel.ac.uk

***Abstract*—Healthcare systems have been supported by technology to help improve the user experience with the entire health system. However, many operational challenges still remain, in particular those related to a unified management of electronic health records (EHR) that could enable multiple doctors to have access to the complete health history of their patient. Blockchain could support unified records, data security and privacy improvement and insurance decisions/transactions making it an effective solution for the above mentioned healthcare technology challenges. The main contribution of this paper is providing preliminary results of a literature review on the adoption of blockchain to support the management of EHR in health systems - along with the benefits and challenges.**

***Index Terms*—Blockchain, EHR, Healthcare, Medical Records.**

## I. Introduction

Public health systems world-wide are currently struggling to deliver core public health services - vaccinations, syndromic and disease surveillance, maternal and child health. Several of those systems have bordered the collapse due to high expenses, large-scale dimensions, and often scarce resources [1], [2]. Unfortunately, the demand is often larger than the value received from social security and private plans. Hence, there is an imminent need to build system resiliency in anticipation to a rapidly growing number of significant stressors and threats to public health and social stability in the coming years.

Healthcare data are the most valuable asset of any healthcare system's intelligence. Most of the time, these data are scattered across different systems and sharing them is influential for establishing an effective and cohesive healthcare system. For example, a patient could visit different doctors in different medical networks for different symptoms, and it would be beneficial for each doctor to see the patient's entire history. Under the current circumstance, a doctor could have a rejected access to the data hosted by other institutions without a mutual sharing agreement for personal health information (PHI). Also, a centralized hosting location of data (e.g., cloud-based solution) can be a single point of a security attack [2]. Anecdotal evidence from recent years shows that healthcare data continues to be a lucrative target for data breaches, thus causing patients to be exposed to economic threats as well as possible social stigma and mental anguish [2].

Cross-institutional sharing of PHI is also complicated due to the demand of a high level of interoperability. As a consequence, data are not always accessible to a provider even when permission is granted [3]. In an ideal world, patients should not only own their own medical records but also be able to control and share their own data without compromising security and privacy. Polls[1] show that about 90% of Americans valued online access to their health records.

With growing recognition of the distributed nature of health services and health records, blockchain technology has recently reached the impetus of the healthcare domain to accommodate the electronic health records (EHR). Starting from Summer 2017, healthcare giants have been involved in blockchain, whether in joining consortium efforts like Hyperledger[2] or developing their own services and products. In parallel, the number of publications in scientific databases have also grown, highlighting the potential of blockchain to improve transparency and security at the sharing of health records.

The main goal of this work is to develop an understanding of the scenarios that involve deploying blockchain for EHR, the benefits that arise from this incorporation and the challenges in such a context. To fulfill the objectives, we formulated two main research questions:

- RQ1. What are the present scenarios and advantages in discussion for the potential usages of blockchain for EHR?
- RQ2. What are the challenges of incorporating blockchain for EHR?

We conducted a search in January 2019 on the potential of blockchain for healthcare systems. We utilized PennState

[1]https://www.healthit.gov/ - The value of consumer access use of online health records.

[2]https://www.hyperledger.org/

LionSearch[3] tool to look for manuscripts using the string ((“Blockchain” OR “Hyperledger”) AND (“Medicine” OR “Healthcare” OR “Nursing”)). LionSearch is an integrated search engine which provides results integrated from over 950 database / search engines, including over 80 databases for healthcare discipline and over 15 for computer / software / information science and engineering. We provide a comprehensive overview of the process we followed in conducting the systematic literature review (SLR) through the link: https://goo.gl/ip95Cm. In this paper, we present a pragmatic view from this search focusing on the potential of blockchain for EHRs to answer the above two questions.

The remainder of this paper is structured as follows: Section 2 provides a background on blockchain. Section 3 provides a brief overview of extracted studies on blockchain for EHRs along with the advantages. Section 4 discusses the challenges that face incorporating blockchain in action, while Section 5 provides the concluding remarks.

## II. Blockchain: Background

Blockchain is an ascending technology that consists in a *append-only* distributed ledger. New entries are added exclusively by appending them at the end of the ledger, the ledger is built as a chronological chain of blocks; hence its name. A blockchain technology is iconically characterized as being (i) ***immutable***, (ii) ***decentralized***, and (iii) ***consensual***, explained as follows. Blockchain is a block hosts with a time-stamped set of transactions that are bundled together. Each new block is linked to its preceding block. Combined with cryptographic hashes, this time-stamped chain of blocks provides a hopefully immutable record of all transactions in a network, from the genesis block until the last / most current block. This is in contrast with a traditional relational database where data can be deleted or modified, there is no administrator permissions within a blockchain that allow for deleting or editing of the recorded data.

A blockchain comprises a set of nodes without a pre-existing trust relationship and are connected through a peer-to-peer network [3]. Each node will host the same exact copy of a blockchain creating a decentralized structure. But for such a structure to be useful, there must exist some mechanism by which the nodes can mutually reach a consensus on the next valid block in the chain to be added. The consensus mechanisms are protocols that make sure all nodes (devices on the blockchain that maintains the blockchain and (sometimes) processes transactions) are synchronized with each other and agree on which transactions are legitimate and added to the blockchain. These consensus mechanisms are crucial for a blockchain in order to correctly work. Some of the deployed schemes for establishing such a distributed consensus include: Proof of Work, Proof of Stake, Proof of Capacity, Proof of Human-Work, Proof of Activity and Proof of Elapsed Time.

In addition to ***decentralization***, ***consensus*** and ***immutability***, a blockchain network also has two additional key characteristics: (iv) ***Provenance*** and (v) ***finality***. Provenance comprises the support for participants of the network to know where the “asset” came from and how its ownership has changed over time; while finality refers to a single and shared ledger providing one unique place to support one to determine the ownership of an asset or the completion of a transaction.

A blockchain can also use smart contracts, which serve as agreements or a set of rules that govern a business transaction.

A blockchain can be both permissionless or permissioned. A permissionless (public) blockchain entitles anyone to join the network. A permissioned (private) blockchain, requires a pre-verification of the participating parties which are known to each other within the network. The choice between the two types is mainly driven by the whether an application can ‘commoditize’ the trust. Bitcoin and Ethereum are examples of permissionless blockchain facilitating parties to transact without necessarily having to verify each other’s identity. On the other hand, EHRs, for example, is an ideal use case for permissioned blockchains. One would not want non-vetted companies participating in the network.

## III. Overview on Blockchain-Based Studies for EHRs and Advantages

Resulting from the SLR process that we conducted on blockchain for healthcare systems (https://goo.gl/ip95Cm) were 52 studies which were analyzed as part of this study. Incorporating blockchain to manage healthcare records was the most popular use case, with 34 studies contributed to the literature discussion and 13 studies presented an innovative application implementation in support of this use case. We provide the complete list of these 34 studies along with a mapping through the link: https://goo.gl/HTQdJ1.

*Preliminary results.* We obtained evidence from most of the studies endorsing that the inherent five characteristics of blockchain fosters the construction of a single shared ledger to (i) store, (ii) share, and (iii) exchange patients’ medical data history among stakeholders while (iv) mitigating the traditional security risks due to the centralization nature of a traditional database or cloud environment.

The 13 reported platforms range from addressing generic health records (e.g., [2], [4]) to more pragmatic ones targeting specific population of patients or medical specialties. For example, in [3], Cichosz et al. presented a blockchain-based platform for sharing healthcare data of Diabetes patients among multiple entities using NEM blockchain[4] which supports multi-signatures enabling several administrative entities the access and control of one data account.

“Healthcoin”[5] is another specialized blockchain based platform to manage and reward Type-2 diabetes prevention. Users interact with the system by submitting their biomarkers into the blockchain. If the biomarker shows improvement, the system awards the patient with digital tokens (“healthcoins”)

[3]http://psu.summon.serialssolutions.com

[4]https://nem.io/

[5]https://healthcoin.com/

which can be applied towards government tax breaks and/or discounts on multiple fitness brands.

Another instance of a specialized blockchain-based platform was presented in [5] describing a ledger that would enable patients free access to their medical image data in a secure manner without requiring a third party administrator. While the actual radiological images are not stored inside the chain due to their large size; a block transaction links a public key to a uniform resource locator (URL) to establish a source of medical imaging data.

Tung et al. presented a similar specialized blockchain-based system for dermatology in [6] to preserve dermatology-related images. Encrypted images are to be stored in blockchain in this case though, with images ownership and locations encoded as transactions and in which patients can access and selectively share medical records using a private digital key.

In collaboration with Stony Brook University Hospital, Dubovitskaya et al. developed a framework on managing and sharing Electronic Medical Records (EMR) for cancer patient care [7]. Since blockchain eliminates the middleman, the proposed framework aims to reduce cost, decrease the turnaround time for cancer patient EMR sharing, and improve medical care decision making.

Internet of Things (IoT)-based healthcare systems are also becoming widely popular to collect remote patient's data in various settings. For example, using analytics on aggregated data and then upon reporting this information to caregivers so that an action is taken, such as shutting down a faulty medical device or changing drug dosage. While privacy is a major concern when using IoT systems [8], augmenting blockchain with sensors and IoTs technologies to support real-time patient monitoring has the potential to automatically notify, in a HIPAA compliant manner, any security vulnerabilities that are associated with remote patient monitoring. This was discussed and presented through a system implementation based on private blockchain based on the Ethereum protocol in [9].

While none of the extracted studies provided an actual validation on a large-scale in practice, there are other projects that are currently in development / validation phase worth mentioning. One implementation example is Guardtime[6], a blockchain-based framework to validate patient identities[7]. Guardtime was created by a Netherlands based data security firm in partnership with the government of Estonia. A smartcard that links EHRs data to an individuals blockchain-based identity was issued to all citizens. A second EHR-related implementation which was tested as a proof of concept is MedRec[8] [10]. MedRec is a project that was initiated between MIT Media Lab and Beth Israel Deaconess Medical Center and it provides a decentralized approach in which the permissions, data storage location, and audit logs are maintained in the blockchain, while all healthcare information remains in the already pre-existing EHR systems. A third EHR project is UK's first trial of blockchain which commenced in July 2018 as a prototype at a southwest London general practice group [11] allowing Medical-chain to gather feedback from doctors and patients that they will use to refine the system before its global launch. Well known companies, such as Deloitte and Accenture, have also been involved in designing blockchain enabled technology for health care data and medical records management.

[6]https://guardtime.com/

[7]https://cointelegraph.com/news/estonian-government-adopts-blockchain-to-secure-1-mln-health-records

[8]https://medrec.media.mit.edu/

## IV. Challenges in Incorporating Blockchain for EHRs Systems

Despite the above advantages, Blockchain will not offer the complete answer for all tribulations of EHRs Systems in its current state. More specifically, we extracted four challenges that we discuss herein:

**Scalability and Performance**: While we could envision the use case of storing the entire EHRs within a blockchain, large medical files (e.g. X-ray and ECG) are too large for direct storage. This challenge was discussed in [3] and [12] and continues to remain a challenge.

In addition, within a blockchain deployment, the decentralization, consensus and provenance features imply that all blocks should be stored on every participating client node within a system. As the size of data will be on constant increase, a demand on every participating node will also increase in order to provide the necessary scalability. To illustrate this scalability issue, a miners full participation in the Bitcoin network requires the miner to download the entire Bitcoin ledger, which totaled over 184 gigabytes at the end of Q3 2018. In addition, the maximum transaction validation within the Bitcoin network is at 7 transactions per second, which increases the possibility of a performance bottleneck. The blockchain-based platform that holds significantly larger volumes of data has to be proven in production environments as of yet [12]. In [3], a possible solution to this challenge proposed to store large collection of medical data off the chain in a data repository called a "data lake". This would still be secure as the blockchain layer would enforce the access control policy. In this framework, "the patient would still have control of who has access to the personal data in the data lake because the data would not be readable without the decryption key, which is stored on the patient's blockchain account" [3].

**Usability**: The cryptographic concepts of Blockchain transactions will be unfamiliar to most people. In the context of medical records sharing, the proposed schemes from the extracted studies require patients to manage their key pairs (public / private) in order to provide cryptographic signatures, and authorize access to their medical data. That said, the fundamental complexity of managing the keys should be concealed behind web and / or mobile application with a user-friendly interface [3]. But this also opens the door to a potential security threat that we will discuss next. Self-governance poses another challenge if the patient is unable to approve necessary access permits. This may occur from simply the loss of personal keys to an acute critical illness such as Alzheimer's disease. Also, in case of an emergency,

the medical data should be accessed to a medical staff by invoking a procedure using a trusted party (e.g., governmental organization, or a close relative).

MIT Media Lab, examined digital certificate implemented with the blockchain technology. Some lessons learned in its first experiments include: "it is much more difficult to manage public / private keys to authenticate both issuer and recipient, hence establishing a wallet that maintains certificates; as Bitcoin holds money, may be an alternative" [12].

**Secure Identification**: In healthcare, the need to match patients to their care records across disparate healthcare provider backends (hospital EHRs, HIEs, labs, etc.) is critical and non-trivial. In the US, the Centers for Medicare & Medicaid Services (CMS)[9] has placed much greater emphasis on healthcare interoperability with its "Promoting Interoperability Program", intended to make patient records access to / from stakeholders easier. Startups, e.g. digitalhealthcare.io[10], are spending resources trying to help resolve some of these very same interoperability issues. These innovations and policy changes, while positive, don't reach far enough the upstream to resolve the question: How do we know who is accessing these patient records in the first place? Who is the real endpoint? It is all about identity, and in fact, within the domain of blockchain technologies, identity management is clearly an important component. Through a variety of related technologies, we are able to associate a user's device (e.g., smartphone) to a uniquely-signed and crypto-secure digital wallet. So to complete this technology we need to be absolutely certain that it is John Doe's smartphone that just extracted tokens from Jane Doe's digital wallet. But smartphones and digital wallets are not people. They are proxies at best, and are prone to failure, get stolen, and sometimes just plain get lost. The integration of unobtrusive biometrics that don't infringe on privacy regulations on the top of a blockchain could be a start to better defining the effect of the unidentified, uninsured patient on overall healthcare expenditures.

**Lack of Incentives and Willingness to Adopt**: Creating a very large network of connected nodes is creating a major monetarily driven challenge. For example, very recently EHR systems were built and cost tens of billions of dollars, and very recently, many large health systems, incentivized by the governments worldwide, invested in building commercial EHR systems [9]. To request for an instant replacement of the current record system with a digital ledger seems to be irresponsible spending on the behalf of tax-payers and will be a disservice to the medical field. On the other hand, for success at maintaining the integrity of the consensus algorithm and to provide the minimum number of validation signatures it is crucial to have a sufficient number of nodes online at any time. Instead, to improve this situation, blockchain would play a more supplemental role and not completely replace the current systems. For example, in each of these nodes would be kept a small amount of descriptive transnational data about particular patient's information or performed procedure while the rest of the pathology results would be kept off of the blockchain. The link embedded in a block would act as a pointer to an off the blockchain API that allow access to the entire test results.

The "immutabilty" characteristic of the blockchain can also be in conflict with existing legislations such as the new European GDPR[11] which aims to give all citizens the ability to govern their personal data including the right for every citizen to request an institution to delete his / her personal data.

[9]https://www.cms.gov/

[10]https://digitalhealthcare.io/

## V. Final Remarks

This paper presented a discussion on the adoption of blockchain to support software-intensive healthcare systems. Preliminary results of a literature review show that, despite the advances that have been achieved, many challenges still remain to make blockchain a panacea for managing EHRs. We have reported the set of platforms that have been specially created and tailored for health systems and EHRs purposes, besides pointing for future directions of research. In a forthcoming paper, we intend to extend the results and provide deeper details on the architectures of the platforms and the challenges to address all the inherent characteristics of blockchain on those systems.

## References


[1] K. Walshe and S. M. Shortell, "When Things Go Wrong: How Health Care Organizations Deal With Major Failures," *Health Affairs*, vol. 23, no. 3, pp. 103–111, 2004.

[2] X. Yue, H. Wang, D. Jin, M. Li, and W. Jiang, "Healthcare Data Gateways: Found Healthcare Intelligence on Blockchain With Novel Privacy Risk Control," *Journal of Medical Systems*, vol. 40, no. 10, 2016.

[3] S. L. Cichosz, M. N. Stausholm, T. Kronborg, P. Vestergaard, and O. Hejlesen, "How to Use Blockchain for Diabetes Health Care Data and Access Management: An Operational Concept," *Journal of Diabetes Science and Technology*, vol. 13, no. 2, 2018.

[4] K. Fan, S. Wang, Y. Ren, H. Li, and Y. Yang, "MedBlock: Efficient and Secure Medical Data Sharing Via Blockchain," *Journal of Medical Systems*, vol. 42, no. 8, 2018.

[5] V. Patel, "A Framework for Secure and Decentralized Sharing of Medical Imaging Data via Blockchain Consensus," *Health Informatics Journal*, 04 2018.

[6] J. Tung and V. Nambudiri, "Beyond Bitcoin: Potential Applications of Blockchain Technology in Dermatology," *British Journal of Dermatology*, vol. 179, no. 4, pp. 1013–1014, 2018.

[7] A. Dubovitskaya, Z. Xu, S. Ryu, M. Schumacher, and F. Wang, "Secure and Trustable Electronic Medical Records Sharing Using Blockchain," in *AMIA (American Medical Informatics Association) Annual Symposium Proceedings*, 2017.

[8] P. A. Laplante, M. Kassab, N. L. Laplante, and J. M. Voas, "Building Caring Healthcare Systems in the Internet of Things," *IEEE Systems Journal*, vol. 12, no. 3, pp. 3030–3037, 2018.

[9] K. N. Griggs, O. Ossipova, C. P. Kohlios, A. N. Baccarini, E. A. Howson, and T. Hayajneh, "Healthcare Blockchain System Using Smart Contracts for Secure Automated Remote Patient Monitoring," *Journal of medical systems*, vol. 42, no. 7, 2018.

[10] A. Azaria, A. Ekblaw, T. Vieira, and A. Lippman, "Medrec: Using blockchain for medical data access and permission management," in *International Conference on Open and Big Data (OBD)*, 2016, pp. 25–30.

[11] S. Armstrong, "Bitcoin technology could take a bite out of NHS data problem," *BMJ: British Medical Journal (Online)*, vol. 361, 2018.

[12] S. Angraal, H. M. Krumholz, and W. L. Schulz, "Blockchain Technology: Applications in Health Care," *Circulation: Cardiovascular Quality and Outcomes*, vol. 10, no. 9, 2017.


[11]https://eugdpr.org/